ADOA-ASET

Project Investment Justification

Version 03.31.15

A Statewide Standard Document for Information Technology Projects

Project Title:

ASLD Security and Business Continuity

Agency Name:	**Arizona State Land Department**
Date:	**May 15, 2015**
Agency Contact Name:	**Carolyn Brown**
Agency Contact Phone:	
Agency Contact Email:	

I. Project Investment Justification (PIJ) Type*

☐ **Yes** ☒ **No** Is this document being provided for a Pre-PIJ / Assessment phase?

If Yes,

Identify any cost to be incurred during the Assessment phase.	**$**
Based on research done to date, provide a high-level estimate or range of development costs anticipated for the full PIJ.	**$**

Explain:

Click here to enter text.

☐ **Yes** ☒ **No** Will a Request for Proposal (RFP) be issued as part of the Pre-PIJ or PIJ?

II. Business Case

*A. Business Problem**

This project is required in order to close current security gaps and in order to meet ASET security standards. ASLD staff met with Tim Guerriero, State Chief Privacy Officer and discussed how this proposal would close identified security gaps including data loss, securing remote access into the environment.

*B. Proposed Business Solution**

Security

The proposed solution is high security architecture with deployment of Citrix NetScaler SDX. SDX is a true service delivery networking platform for enterprises and cloud datacenters and features an advanced virtualization architecture that supports multiple NetScaler instances on a single hardware appliance.

NetScaler provides a security-hardened platform with multiple integrated security capabilities designed to protect against a wide variety of threats and attacks — including denial of service (DoS) and day zero attacks.

Provides the capability to:

- Rewrite OWA access for external users accessing Outlook Web Access
- Proxy access for ActiveSync for external users
- Secure access to users XenDesktop virtual machines from any client or device.

Two-factor authentication would be provided through the use of security tokens to the end clients (mobile & desktop).

Business Continuity server

ASLD is adding a failover solution server in the event production servers should lose availability due to unscheduled downtime this server will ensure the system remains active until such time as the system is fully restored.

Cisco UCS B460 M4 Blade Server:

- Provide redundancy to ensure business continuity due during any issues that may arise.

*C. Quantified Benefits**

x	Service enhancement
	Increased revenue
	Cost reduction
x	Problem avoidance
x	Risk avoidance

Explain:

Providing a failover server provides uninterrupted service in the event of unplanned system disruption.

Problems and risks will be avoided with increased end to end web security and two factor authentication. Less risk results in service enhancement as ASLD network will be protected from a wide variety of attacks.

III. Technology Approach

*A. Proposed Technology Solution**

Cisco UCS B460 M4 Blade Server:
This will also act as host and backup server for our CITRIX desktop environment.

- Provide redundancy to ensure business continuity during any issues that may arise.
- Mirror of production system that provides end user system and applications
- Uncompromised expandability, versatility, and performance.
- Offers advances in fabric-centric computing, open APIs, and application-centric management, and uses service profiles to automate all aspects of server deployment and provisioning.

NVIDIA Grid Technology:

- Cloud server efficiency by offloading the CPU from encoding functions
- Power efficiency.
- 24/7 reliability.

ELA2 Netscaler SDX:
END-TO-END WEB SECURITY
Iron-clad security is a key objective for any network. NetScaler provides a security-hardened platform with multiple integrated security capabilities designed to protect against a wide variety of threats and attacks — including denial of service (DoS) and day zero attacks. These integrated capabilities include:

- FIPS compliance — through a line of appliances with more than 4.5 Gbps SSL throughput
- Secure remote access — using built-in SSL VPN that encrypts data and provides secure remote access for all users

- DNSSEC protection — to provide authentication of DNS data and denial of existence, plus ensure data integrity
- Application firewall — with built-in intelligence and proactive, app-level security

EZ Netscaler Application Firewall

Two-factor authentication –User authentication takes place on the NetScaler. The users credentials are forwarded using the NetScalers IP address, or NSIP, into the internal authentication services, (Active Directory) where they will be validated (or not). Once validated and still part of NSIP, two factor authentication using SMS passcode tokens for example can be initiated. This way every user will have to fill in his or her username and password plus an additional auto generated token code which will expire every few minutes (configurable), extremely secure.

B. Existing Technology Environment

We are not changing existing technology but augmenting in order to close current security gaps. The NetScaler will be installed into the proposed CISCO UCS network infrastructure identified in the ASLD Refresh PIJ. Current failover solution is IBM system storage TS3310 Tape Library tape backup from SAN storage. Backup server will be retained for tape backup library server

C. Selection Process

Products were reviewed and tested to ensure computability with ASLD infrastructure and provide optimum performance. Quotes were obtained to ensure all proposed technology is in compliance with State contracts and purchasing policies.

IV. Project Approach

*A. Project Schedule**

Project Start Date: Click for date. **Project End Date**: 12/31/2015

B. Project Milestones ***(please note we will provide dates upon project approval)***

Major Milestones	Start Date	Finish Date
Design the installation and migration process	July 1, 2015	Sept 30, 2015
Order project hardware and software	June 19, 2015	June 30, 2015
Install, configure and test server components	July 15, 2015	Dec 31, 2015

C. Project Roles and Responsibilities

Vendor integration services as contracted.

William Reed, the Department's Chief Technology Officer and Information Security Officer will have the overall responsibility for the design and implementation of this project.

Arthur Sarumov, ITS 4 EDP Tech Sup Spec II will perform installation and configuration work associated with the blade center and blade servers

Ken Hankish, ITS 4 Network Spec II will perform installation and configuration work associated with the directory services and other IT management servers

V. Risk Matrix, Areas of Impact, Itemized List, PIJ Financials

VI. Project Approvals

*A. Agency CIO/ISO Review and Initials Required**

Key Management Information	Yes	No	Inits
1. Is this project for a mission-critical application system?		**N**	
2. Is this project referenced in your agency's Strategic IT Plan?	**Y**		
3. Have you reviewed and is this project in compliance with all applicable Statewide policies and standards for network, security, platform, software/application, and/or data/information located at https://aset.az.gov/resources/psp? If **NO**, explain in detail in section **"VIII. Additional Information"** below.	**Y**		
4. Will any PII, PHI, or other Protected Information as defined in the 8110 Statewide Data Classification Policy located at https://aset.az.gov/resources/psp be transmitted, stored, or processed with this project? If **YES, the Protected Data section under "VII. Security Controls" below will need to be completed.**		**N**	
5. Will this project migrate, transmit, or store data outside of the agency's in-house environment or the State Data Center? If **YES**, **the Hosted Data section under "VII. Security Controls" below will need to be completed.**		**N**	
6. Is this project in compliance with the Arizona Revised Statutes and GRRC rules?	**Y**		
7. Is this project in compliance with the Statewide policy regarding the accessibility to equipment and information technology for citizens with disabilities?	**Y**		

*B. Project Values**

The following table should be populated with summary information from other sections of the PIJ.

Description	Section	Number or Cost
Assessment Cost (if applicable for Pre-PIJ)	I. PIJ Type - Pre-PIJ Assessment Cost	**$**
Total Development Cost	V. PIJ Financials tab	**$230,380.89**
Total Project Cost	V. PIJ Financials tab	**352,998.25**
FTE Hours	1000	

*C. Agency Approvals**

Approver	Printed Name	Signature	Email and Phone
Project Manager:	William Reed		
Agency Information Security Officer:	William Reed		
Agency CIO:	Evan Brom		
Project Sponsor:	Evan Brom		
Agency Director:			

VII. Security Controls

Collaboration with the ADOA-ASET Security, Privacy and Risk (SPR) team may be needed to complete this section, which is only required for those projects that involve data that is Protected or Hosted outside of the Agency or State Data Center. Additional information can be found in the NIST FRAMEWORK section under RESOURCES at https://aset.az.gov/resources/psp or you may wish to contact ASET-SPR directly at secadm@azdoa.gov for assistance.

A. Protected Data

Click here to enter text.

B. Hosted Data

☐ Check here if the https://aset.az.gov/arizona-baseline-security-controls-excel spreadsheet is attached. Otherwise explain below what information/ support is needed to complete the spreadsheet and/or why no sheet is attached:

Click here to enter text.

☐ Check here if a Conceptual Design / Network Diagram is attached. Otherwise explain below what information/support is needed to complete the diagram and/or why no diagram is attached:

Click here to enter text.

VIII. Additional Information

IX. Attachments

The following are examples of supporting documents that should be sent as email attachments when required:

A. *Vendor Quotes*
B. *Arizona Baseline Security Controls spreadsheet*
C. *Conceptual Design / Network Diagram*
D. *Other*

X. Glossary

Other Links:
ADOA-ASET Website
ADOA-ASET Project Investment Justification Information Templates and Contacts

Email Addresses:
Strategic Oversight
ADOA-ASET_Webmaster@azdoa.gov